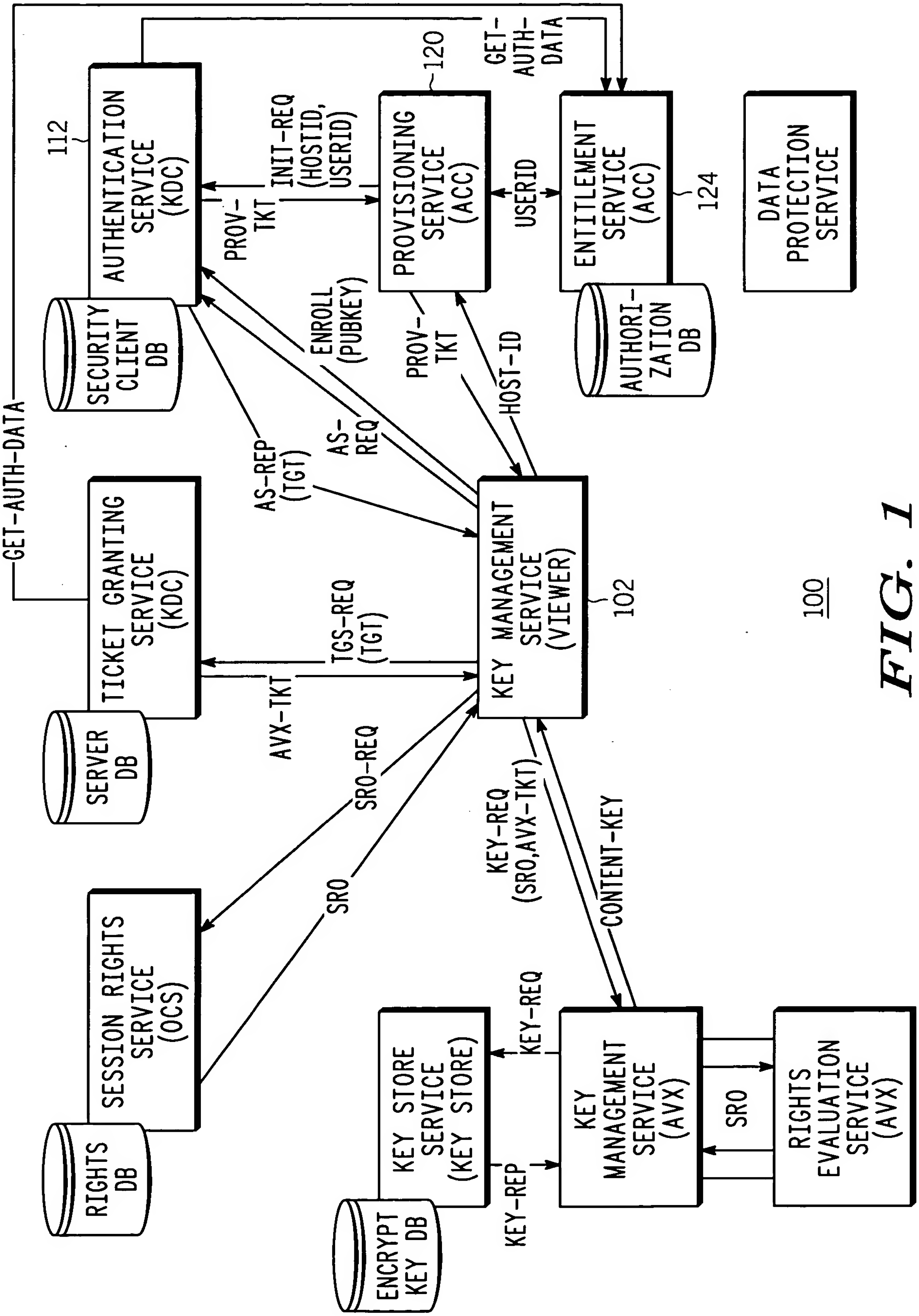
AUTHENTICATION SERVICE (KDC)
112
SECURITY CLIENT DB
PROVISIONING SERVICE (ACC)
120
ENTITLEMENT SERVICE (ACC)
124
AUTHORI-ZATION DB
DATA PROTECTION SERVICE
GET-AUTH-DATA
GET-AUTH-DATA
INIT-REQ (HOSTID, USERID)
PROV-TKT
USERID
ENROLL (PUBKEY)
PROV-TKT
HOST-ID
AS-REP (TGT)
AS-REQ
TICKET GRANTING SERVICE (KDC)
SERVER DB
KEY MANAGEMENT SERVICE (VIEWER)
102
TGS-REQ (TGT)
AVX-TKT
SRO-REQ
SRO
SESSION RIGHTS SERVICE (OCS)
RIGHTS DB
KEY-REQ (SRO,AVX-TKT)
CONTENT-KEY
KEY STORE SERVICE (KEY STORE)
ENCRYPT KEY DB
KEY-REQ
KEY-REP
KEY MANAGEMENT SERVICE (AVX)
SRO
RIGHTS EVALUATION SERVICE (AVX)
100

FIG. 1

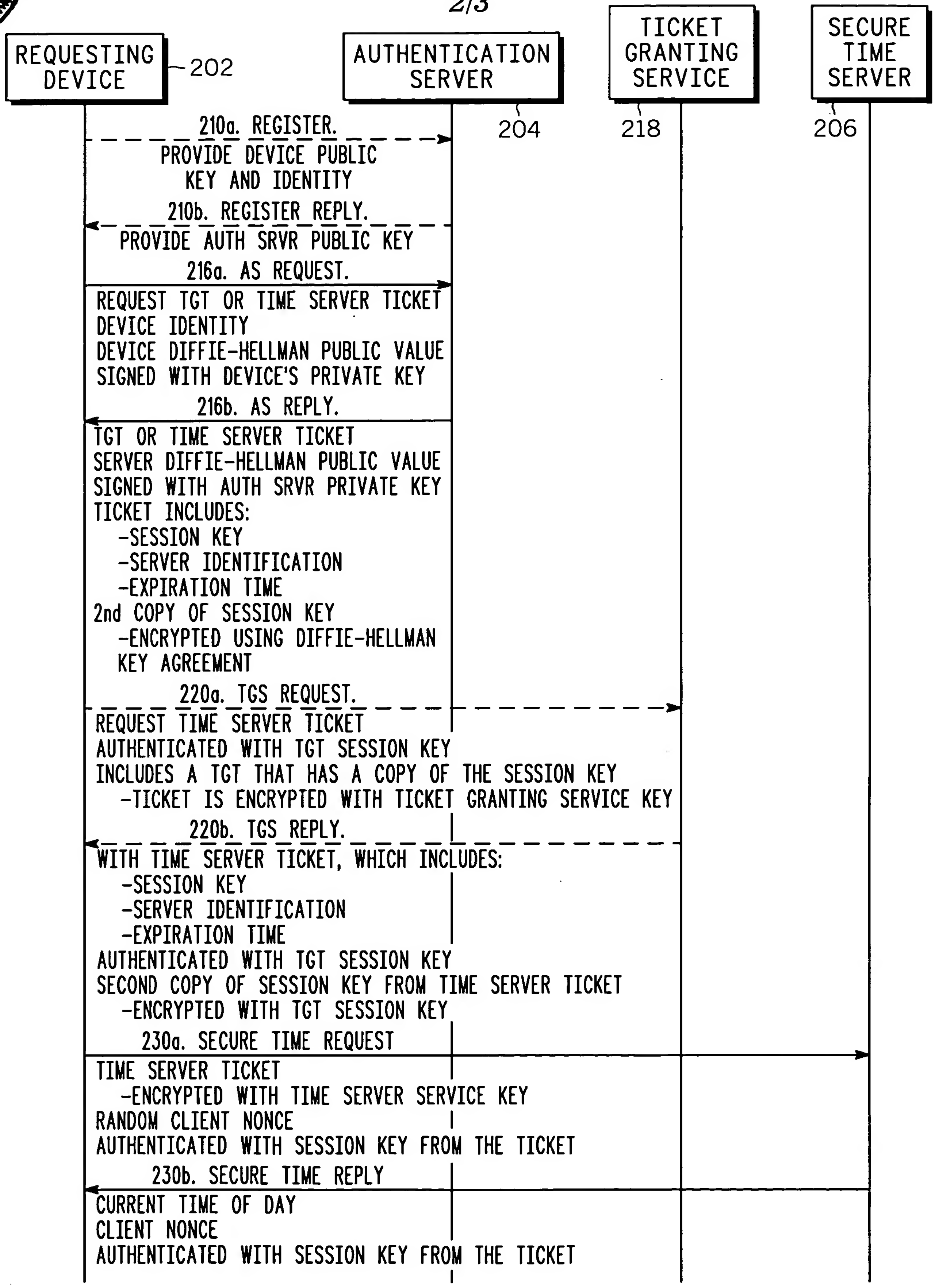
REQUESTING DEVICE
202
AUTHENTICATION SERVER
204
TICKET GRANTING SERVICE
218
SECURE TIME SERVER
206
210a. REGISTER.
PROVIDE DEVICE PUBLIC KEY AND IDENTITY
210b. REGISTER REPLY.
PROVIDE AUTH SRVR PUBLIC KEY
216a. AS REQUEST.
REQUEST TGT OR TIME SERVER TICKET
DEVICE IDENTITY
DEVICE DIFFIE-HELLMAN PUBLIC VALUE
SIGNED WITH DEVICE'S PRIVATE KEY
216b. AS REPLY.
TGT OR TIME SERVER TICKET
SERVER DIFFIE-HELLMAN PUBLIC VALUE
SIGNED WITH AUTH SRVR PRIVATE KEY
TICKET INCLUDES:
-SESSION KEY
-SERVER IDENTIFICATION
-EXPIRATION TIME
2nd COPY OF SESSION KEY
-ENCRYPTED USING DIFFIE-HELLMAN KEY AGREEMENT
220a. TGS REQUEST.
REQUEST TIME SERVER TICKET
AUTHENTICATED WITH TGT SESSION KEY
INCLUDES A TGT THAT HAS A COPY OF THE SESSION KEY
-TICKET IS ENCRYPTED WITH TICKET GRANTING SERVICE KEY
220b. TGS REPLY.
WITH TIME SERVER TICKET, WHICH INCLUDES:
-SESSION KEY
-SERVER IDENTIFICATION
-EXPIRATION TIME
AUTHENTICATED WITH TGT SESSION KEY
SECOND COPY OF SESSION KEY FROM TIME SERVER TICKET
-ENCRYPTED WITH TGT SESSION KEY
230a. SECURE TIME REQUEST
TIME SERVER TICKET
-ENCRYPTED WITH TIME SERVER SERVICE KEY
RANDOM CLIENT NONCE
AUTHENTICATED WITH SESSION KEY FROM THE TICKET
230b. SECURE TIME REPLY
CURRENT TIME OF DAY
CLIENT NONCE
AUTHENTICATED WITH SESSION KEY FROM THE TICKET

FIG. 2

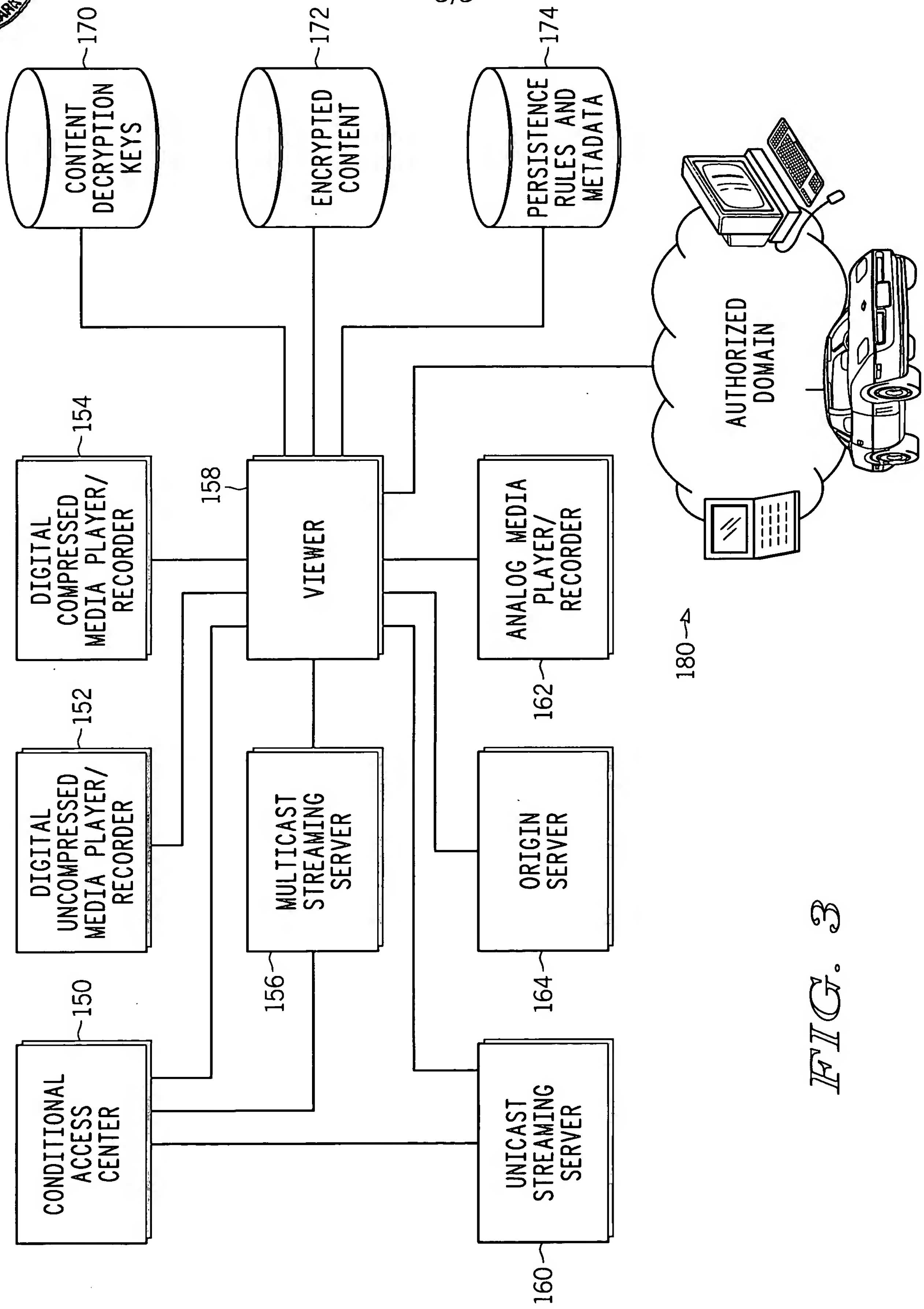
170
CONTENT DECRYPTION KEYS
172
ENCRYPTED CONTENT
174
PERSISTENCE RULES AND METADATA
154
DIGITAL COMPRESSED MEDIA PLAYER/ RECORDER
158
VIEWER
AUTHORIZED DOMAIN
152
DIGITAL UNCOMPRESSED MEDIA PLAYER/ RECORDER
MULTICAST STREAMING SERVER
156
ANALOG MEDIA PLAYER/ RECORDER
162
180
ORIGIN SERVER
164
150
CONDITIONAL ACCESS CENTER
UNICAST STREAMING SERVER
160

FIG. 3